Online Risk-Based Security Assessment

Ming Ni, *Member, IEEE*, James D. McCalley, *Senior Member, IEEE*, Vijay Vittal, *Fellow, IEEE*, and Tayyib Tayyib, *Member, IEEE*

***Abstract*—The work described in this paper was motivated by a perceived increase in the frequency at which power system operators are encountering high stress in bulk transmission systems and the corresponding need to improve security monitoring of these networks. Online risk-based security assessment provides rapid online quantification of a security level associated with an existing or forecasted operating condition. One major advantage of this approach over deterministic online security assessment is that it condenses contingency likelihood and severity into indices that reflect probabilistic risk. Use of these indices in control room decision making leads to increased understanding of potential network problems, including overload, cascading overload, low voltages, and voltage instability, resulting in improved security-related decision making. Test results on large-scale transmission models retrieved from the energy-management system of a U.S. utility company are described.**

***Index Terms*—Cascading, control center, decision making, operations, overload, probabilistic risk, security assessment, uncertainty, voltage instability.**

I. Introduction

IN MANY countries today, the introduction of competitive supply and corresponding organizational separation of supply, transmission, and system operation has resulted in more highly stressed and unpredictable operating conditions, more vulnerable networks, and an increased need to monitor the operational security level of the transmission system. These conditions, brought on by natural load growth coupled with a significant increase in long-distance transmission usage, often result in heavy transmission circuit loadings, depressed bus voltage magnitudes, and closer proximity to voltage instability. As a result, operators are frequently finding that they are required to make complex decisions regarding whether or not to take action in order to alleviate stressed conditions in their networks, and if so, which actions to take and to what extent. Usually, such actions increase the cost of supply, and therefore, the decision-making process requires trading off security against economics. Since this process most often takes place in the control room, we refer to it as control-room security-economy decision making.

Existing energy-management systems (EMS) enable operators and control room engineers to monitor network conditions through supervisory control and data acquisition (SCADA), state estimation, and deterministic contingency analysis. Although useful and necessary, use of these tools in the decision-making process requires a significant amount of subjective assessment regarding questions like: How many overloads or voltage violations are there and how severe are they? How close to voltage instability? Is cascading possible? What is the likelihood of occurrence for each contingency? We believe that risk indices may be used to more efficiently address these types of questions. This paper describes such indices and the computations required to obtain them online. We refer to these computations as online risk-based security assessment (OL-RBSA).

OL-RBSA provides the ability to compute online probabilistic risk associated with conditions up to several hours in the future. A significant advantage of this tool is that distinguishes it from predecessor EMS security assessment technology in that it uses probabilistic modeling of uncertainty. Specifically, this modeling accounts for uncertainty in loading conditions and in outage conditions that, when combined with severity assessment that results from analysis of the power system performance, yields indices that indicate the risk.

One feature of OL-RBSA is that it performs security assessment on a **near-future** condition. This is in distinct contrast to traditional online security assessment, which always performs security assessment on a past condition (i.e., the last state-estimation). The great advantage of this feature is that information on which the decision is based, from the assessment, corresponds to the time frame in which the decision is effective.

In this paper, Section II gives the conceptual thrust of OL-RBSA. Section III provides its computational description. In Section IV, the test results on a large-scale transmission model retrieved from the EMS of a U.S. utility company are described. The benefits of applying OL-RBSA are verified and illustrated by comparing deterministic results in Section V. Section VI summarizes the unique features of OL-RBSA and provides a discussion on the potential application of OL-RBSA in control-room security-economy decision making, and conclusions are given in Section VII.

II. Conceptual Thrust of OL-RBSA

A. Concept of Risk

Our implementation of OL-RBSA includes overload security (flow violations and cascading overloads) and voltage security (voltage magnitude violations and voltage instability). It does

Manuscript received July 17, 2002. This work was supported by the Electric Power Research Institute under Contract WO663101.

M. Ni, J. D. McCalley, and V. Vittal are with Iowa State University, Ames, IA 50010 USA (e-mail: mingni@iastate.edu; jdm@iastate.edu; vvittal@iastate.edu).

T. Tayyib is with the Electric Power Research Institute, Palo Alto, CA 94304 USA (e-mail: TTayyib@epri.com).

Digital Object Identifier 10.1109/TPWRS.2002.807091

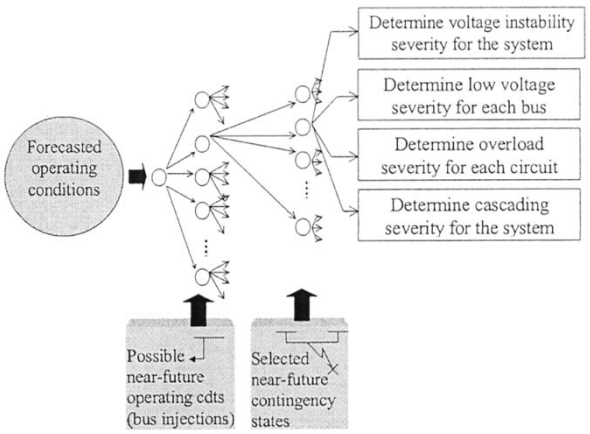

Fig. 1. Illustration of basic OL-RBSA calculation.

not include dynamic security assessment.[1] The risk index is an expectation of severity, computed by summing over all possible outcomes the product of the outcome probability and its severity. In Fig. 1, if we assign probabilities to each branch, then the probability of each terminal state is the product of the probabilities assigned to the branches that connect the initial state to that terminal state.

If we assign severity values to each terminal state, the risk can be computed as the sum over all terminal states of their product of probability and severity, as shown in (1)

$$Risk(X_{t,f}) = \sum_i \Pr(E_i)\left(\sum_j \Pr(X_{t,j}|X_{t,f}) \times Sev(E_i, X_{t,j})\right). \quad (1)$$

Here

- $X_{t,f}$ is the forecasted condition at time t. It is typically predicated on the last state estimation result together with a forecast of how these conditions change during the time between the last state estimation result and t. t is limited by the time associated with the unit commitment and the accuracy of the load forecast.
- $X_{t,j}$ is the jth possible loading condition. It provides that load forecast uncertainty be included in the assessment. $\Pr(X_{t,j}|X_{t,f})$ is the probability of this condition, obtained from a probability distribution for the possible loading conditions. In Section II-C, we introduce a fast calculation procedure to translate the distribution on loading to distributions on performance measures.
- E_i is the ith contingency and $\Pr(E_i)$ is its probability. Here, we assume the existence of a contingency list.
- $Sev(E_i, X_{t,j})$ quantifies the severity, or consequence, of the ith contingency occurring under the jth possible operating condition. It represents the severity for overload, low voltage, voltage instability, and cascading overloads.

[1]Dynamic security assessment (DSA) is not within the scope of this paper, but a modification to the given expression enables DSA applicability. For overload and voltage security, the severity is completely determined once the outaged component and the operating conditions are specified. For DSA, this is not the case because the severity (loss of synchronism at a plant) also depends on additional, but generally uncertain, information pertaining to the contingency, including fault type, fault location on the circuit, and clearing time [1]–[5].

B. Modeling of Severity Function

Severity provides a quantitative evaluation of what would happen to the power system in the specified condition in terms of severity, impact, consequence, or cost. CIGRE Task Force 38.02.21 [6] identified it as a difficult problem in probabilistic security assessment.

We have identified criteria for a good severity function to be used in OL-RBSA. First, the severity function should reflect the consequence of the contingency and loading condition, rather than the consequences of an operator's decision. For example, operator-initiated load curtailment or redispatch reflects the consequence of the operator's decision to interrupt load or modify the dispatch, respectively. Thus, use of a load-interruption based index, such as LOLP or EUE, familiar to planners, or an index based on cost of redispatch, is inappropriate for use in control-room security-economy decision making. This is because the assessment is being used to facilitate the operator's decision making; to construct the index based on load interruption presupposes the very decision the index is supposed to facilitate.[2] Second, the severity for contingencies should reflect consequences that are physically understandable in terms of network parameters by the operator. This criterion ensures that the resulting indices provide engineering insight and intuition to operators with respect to the problems they face. It also rules out the use of an economic severity function for control-room security-economy decision making. Economic-based severity functions, although attractive because they may be easily combined with other economic-based indices, are highly uncertain, and most important, they do not intuitively translate into network performance measures. Third, the severity functions should be tied to deterministic decision criteria, to the extent possible, in order to facilitate the transition that their use requires of operators. Fourth, the severity functions should be simple. Fifth, the severity functions should reflect relative severity between different problems to enable calculation of composite indices. Finally, the severity function should measure the extent of a violation.

In what follows, we describe several severity functions, each of which has strengths and weaknesses with respect to the above criteria. Our basic approach is to use functions of network performance measures.

1) Severity Function for Low Voltage: The severity function for low voltage is defined specific to each bus. The voltage magnitude of each bus determines the low-voltage severity of that bus. We define the following three kinds of severity functions.

a) Discrete Severity Function: Severity is assigned a value 1 if the voltage magnitude is lower than the low voltage rating, and 0 otherwise [see Fig. 2(a)]. Therefore, when discrete severity functions are used, the resulting *risk* computed by (1) reveals the expectation of the number of buses that will have low-voltage violations in the next time period. The advantages of this severity function are that it is simple, no estimation is required, and it enjoys strong coupling with the deterministic approach. Its disadvantage is that it does not reflect the extent of the violation.

[2]The exception to this is when an action such as load interruption occurs automatically and is therefore not a result of an operator's decision.

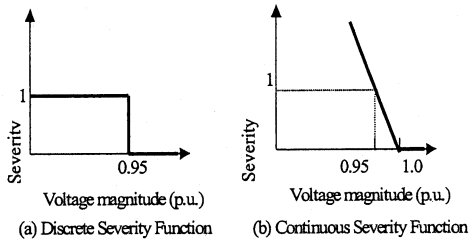

Fig. 2. Severity function for low voltage.

b) Percentage of Violation Severity Function: This severity function uses the percentage of violation to define the severity of a low-voltage problem. The severity function is defined as

$$Sev_{lv}(V_j) = \begin{cases} \dfrac{0.95 - V_j}{0.95}, & V_j \le 0.95 \\ 0, & V_j > 0.95. \end{cases} \quad (2)$$

Although this severity function does measure the extent of the violation, it does not compose with risk indices for other security problems.

c) Continuous Severity Function: The continuous severity function for low voltage is illustrated in Fig. 2(b). For each bus, the severity evaluates to 1.0 at the deterministic limits (0.95 p.u.) and increases linearly as voltage magnitude falls below the limit. This severity function measures the extent of the violation, and it is composable. In addition, its use results in nonzero risk for performance close to, but within a performance limit, reflecting the realistic sense that such a situation is, in fact, risky.

2) Severity Function for Overload: The severity function for overload is defined specific to each circuit (transmission lines and transformers). The power flow as percentage of rating (PR) of each circuit determines the overload severity of that circuit. The discrete and continuous severity functions for overload are shown in Fig. 3, and the percentage of violation severity function is defined as

$$Sev_{ol}(PR_k) = \begin{cases} PR_k - 1.0, & PR_k \ge 1.0 \\ 0, & PR_k < 1.0. \end{cases} \quad (3)$$

3) Severity Function for Voltage Instability: The severity function of voltage instability is a system severity function rather than a component severity function. We use the loadability corresponding to the system bifurcation point to determine the voltage instability severity. Here we define "$\%margin$" as the percentage difference between the forecasted load and loadability, as expressed in (4)

$$\%margin = \frac{Loadability - (Forecasted\_Load)}{(Forecasted\_Load)} * 100\%. \quad (4)$$

For the voltage instability problem, we use "$\%margin$" to define two kinds of severity functions: discrete and continuous. They are illustrated in Fig. 4. If $\%margin$=0, a voltage collapse will occur for the given contingency state at the particular operating condition. The actual effects of such an outcome are quite difficult to identify, as the system dynamics play a heavy role. Nonetheless, it is safe to say the consequence is very severe and

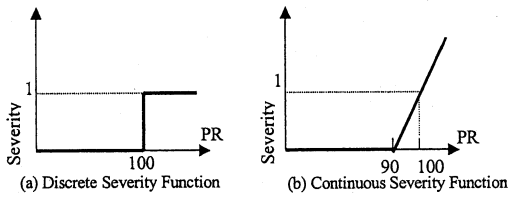

Fig. 3. Severity function of overload.

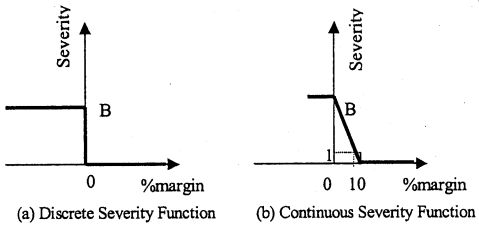

Fig. 4. Severity function of voltage instability.

generally unacceptable under any condition. We therefore assign severity $\boldsymbol{B}$ to it, where $\boldsymbol{B}$ depends on the decision maker's valuation of a voltage collapse relative to a violation of the deterministic criteria.[3]

4) Severity Function for Cascading Overloads: "Cascading" is a sequential succession of dependent events. The types of events that may contribute to cascading phenomena vary widely. In this paper, we only consider the cascading caused by high flows, and we refer to the corresponding index as "cascading overload risk." This index reflects an important kind of security risk that is not captured by our other indices. We make the following assumption for the purpose of assessing the cascading overload security: *A circuit will be outaged if its MVA flow exceeds* $\boldsymbol{K}$ *times its emergency overload rating.* A conservative choice of $\boldsymbol{K}$ is 1.0, reflecting that a circuit outages when its flow exceeds its emergency overload rating. To remain consistent with our first requirement on severity functions, the assessment is made assuming no operator action (such as redispatch) occurs.

Our analysis algorithm is simple. Given a contingency state (the post-contingency power-flow solution for a certain contingency in the contingency list)

1) identify all circuits having flow exceeding $\boldsymbol{K}$ times its emergency overload rating;

2) remove these circuits, and resolve the power flow;

3) repeat Steps 1) and 2) until one of the following conditions are met:

a) no circuits are identified in step 1).
b) the power-flow solution procedure diverges in step 2).
c) the procedure exceeds a prespecified number of iterations of steps 1) and 2).

The *cascading level* is the number of iterations of steps 1) and 2). Severity index depends on the stopping criteria in step 3).

- If the algorithm terminates as a result of criterion 3-a, then the severity function is given as a function of the

[3]The severity functions are, in fact, value functions, in that they assign a unique number to each consequence [7]. Value functions like this are also used to quantify severity for probabilistic risk assessment within other industries as well, and a good example is process control [8]–[10].

total number of outaged circuits found in level 2 or higher. Therefore, the severity function used for cascading overload risk is a linearly increasing function with the number of outaged circuits. We do not include outaged circuits in level 1 because this impact is reflected in the overload risk index.

- If the algorithm terminates as a result of criterion 3-b or 3-c, then we assume the system collapses. Thus, we assign the same severity as for voltage instability B.

Whereas the overloading risk index reflects the number of and the extent to which level 1 circuits are overloaded following an initial contingency, the cascading risk index reflects the number of circuits that will cascade if the level 1 overloaded circuits are opened.

C. Modeling of Uncertainty

From (1), we can see that two kinds of uncertainties are considered, one is uncertainty of contingencies ($\Pr(E_i)$), and the other is uncertainty of operating conditions ($\Pr(X_{t,j}|X_{t,f})$).

1) Uncertainty of Contingency: In traditional deterministic security assessment, the impact of each contingency is considered, but not the probability of each contingency. Decisions based on deterministic assessment are driven by the most severe credible contingency. This results in an inconsistent action trigger and selection of less effective actions [11]. Therefore, we characterize contingency uncertainty using probabilistic representation. In (1), $\Pr(E_i)$ is the probability of contingency i in the next time interval. The events E_i are assumed to be Poisson distributed so that

$$\Pr(E_i) = \left(1 - e^{-\lambda_i}\right) * \exp\left(-\sum_{j \neq i} \lambda_j\right). \tag{5}$$

Here, λ_i is the occurrence rate of contingency i per unit time.

2) Uncertainty of Operating Condition: We desire to evaluate the security level at a future time t given that the forecasted operating condition in time period t is $X_{t,f}$. The operating condition, in terms of the load and dispatch, of the future time t is uncertain. It is appropriate to model the probability distribution of X_t given $X_{t,f}$ with a normal distribution having a mean equal to the forecast. Under this assumption, the bus voltage magnitudes and branch flows of X_t follow the multivariate-normal (MVN) distribution [12], [13], and system loadability (for measuring voltage instability performance) follows the normal distribution. The task here is to give the probability distributions of voltage magnitude $\Pr(V|E_i, X_t)$; branch flow $\Pr(P|E_i, X_t)$; and loadability $\Pr(L_m|E_i, X_t)$, where E_i is a contingency state.

We capture the uncertainty in operating conditions by identifying specific operating parameters that cause this uncertainty. These include load distribution factors among load buses, load power factors, and generation participation factors. We assume that these parameters are random in the future, and that they follow an MVN distribution around their expected values, and their deviations, although random, are small such that linear approximation of these measures (voltage magnitude, branch flow, and loadability) with respect to these parameters is valid.

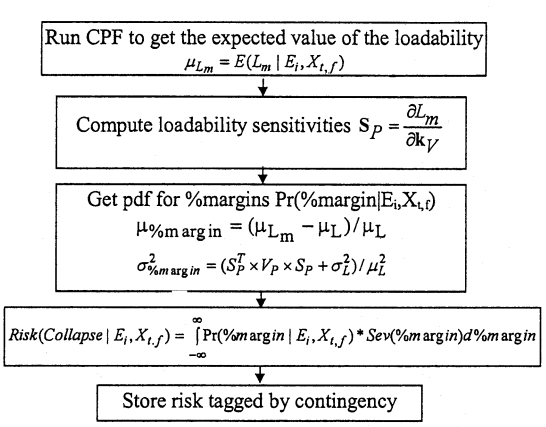

Fig. 5. Voltage instability risk calculation for a given contingency.

We denote these random parameters as $\underline{K}_P$, their expectation as $E(\underline{K}_P)$, and their variance-covariance matrix as V_P. Denote specific performance measures (loadability, voltage magnitude, and branch flow) as Y_t and the sensitivity of performance measures with respect random parameters as $\underline{S}_P$. Then, it can be proven [21] that Y_t, a linear function of the MVN distributed $\underline{K}_P$, also follows a Normal distribution:

$$Y_t \sim Normal(E(Y_t), \underline{S}_P^T \times V_P \times \underline{S}_P). \tag{6}$$

In (6), the expectation of Y_t and its sensitivities can be obtained from the standard load-flow Jacobian (for bus voltage magnitude and for line loading) and the continuation power flow (CPF) [14]–[20] (for voltage instability).

III. OL-RBSA Calculation Structure

The calculation of OL-RBSA includes two main steps.

1) Calculate the risk indices for each contingency. In this step, the risk indices of each contingency are calculated for a given contingency state (i.e., a post-contingency power-flow solution). Therefore, contingency uncertainty has no effect in this step.

2) Combine the risk of all contingencies. In this step, for each security problem, the risk indices of each contingency are weighted by the corresponding probability of contingency and then summed, providing the total risk of each security problem. In this step, the uncertainty of the contingency is considered.

Fig. 5 illustrates the procedures for computing voltage instability risk indices for a certain contingency, where L_m is the loadability;, μ_L denotes the expected load level; and μ_{Lm} denotes the expected loadability. Procedures for computing risk indices associated with low voltage, overload, and cascading overload are similar.

For a given contingency, we use the CPF to obtain μ_{Lm}. The variance of the loadability is calculated by the method described in Section II-C. To quantify the voltage instability risk, the $\%margin$, which is the difference between the forecasted load and loadability, is used. The probability distribution function of $\%margin$ is given in the third block. Then we use the discrete and/or continuous severity function to calculate the voltage instability risk of the system under this contingency.

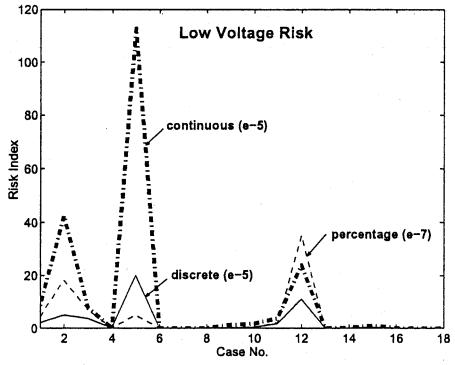

Fig. 6. Low-voltage risk of serial cases.

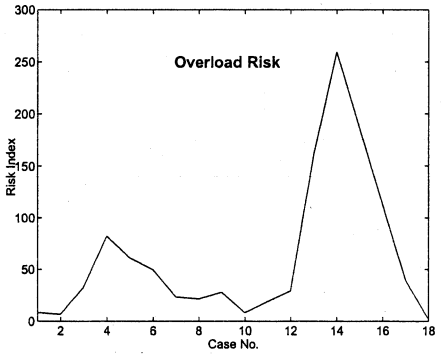

Fig. 7. Overload risk of serial cases.

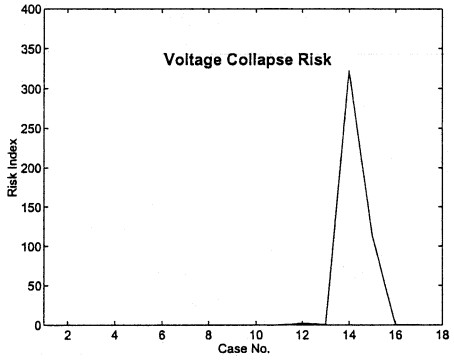

Fig. 8. Voltage instability risk of serial cases.

IV. Numerical Results

In this section, the results of OL-RBSA from 18 cases are given. These cases represent two days' (July 3, 2000 and July 6, 2000) over certain hours (6:00 A.M., 8:00 A.M., 10:00 A.M., 12:00 P.M., 2:00 P.M., 4:00 P.M., 6:00 P.M., 8:00 P.M., and 10:00 P.M.). These cases were retrieved from one utility company's EMS. The model includes all of the generators, transformers and transmission lines over 49-kV voltage level and also some components in surrounding areas. The system has approximately 1600 buses and 2600 circuits. The contingency set used in this test contains 17 contingencies: One N-3, two N-2 and 14 N-1, consisting of generator, transmission line, and transformer outages. This set was chosen because it serves as a reference set for the utility; our software allows for a larger number of contingencies as well.

Using the 18 serial cases, we calculate the risk indices by OL-RBSA. The results are shown using risk-time curves. From these curves, we can see how the indices vary with time.

A. Low-Voltage Risk

The total low-voltage risks of the system for the 18 cases are shown in Fig. 6.

These curves disclose that cases 2, 5, and 12 are the three most risky cases in terms of low voltage. Observations about these figures are as follows:

- When using the discrete and continuous severity function, the most risky case is case 5. However, the second most risky cases are not the same; for discrete severity function, it is case 12, while for continuous severity function, it is case 2. This is because the discrete severity function only captures the violation of the bus voltage, while the continuous severity function reflects the extent of a violation and also nonzero severity when attributes (voltage magnitude, circuits flow, and loadability) are close to a violation.
- When using the percentage of violation severity function, the most risky case is case 12 and the second most risky case is case 2. This (case 12, case 2) ordering differs from the (case 5 and case 12) ordering of the discrete severity function because the percentage of violation severity function captures the extent of a violation, and the discrete severity function does not. This (case 12, case 2) ordering is also different from the (case 5, case 2) ordering of the continuous severity function because the continuous severity function reflects nonzero severity when performance measures are close to a violation, and the percentage of violation severity function does not.

The results show that when we adopt different severity functions, the conclusions may be different. So the selection of an appropriate severity function is a crucial issue in risk calculation. From the result presented before, we can see that the continuous severity function is the most desirable, as it can capture effects that the other two severity functions cannot. So in what follows, we only give the risk indices obtained by using the continuous severity function.

B. Overload and Voltage Instability Risk

The total overload risks and voltage instability risks of the system for the 18 cases are shown in Figs. 7 and 8, respectively, using the continuous severity function. High risk for case 14 is observed for both overload and voltage instability.

C. Cascading Risk

The total cascading risks of the system for the 18 cases are shown in Fig. 9. From this figure, we see that cases 12 to 16 have the most serious cascading problem among the 18 cases.

V. Benefits of Using OL-RBSA

In this section, we compare the information obtained from the OL-RBSA indices to several other indices that reflect the thinking embedded in traditional security assessment, for low-voltage and voltage instability. We provide a convenient summary regarding definition of these indices in what follows. The

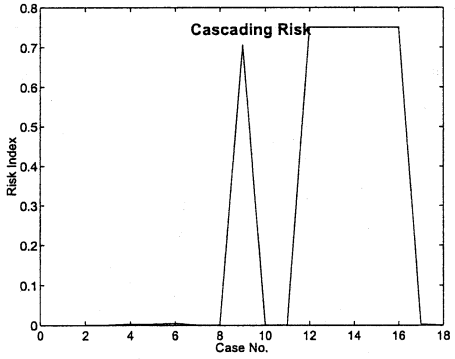

Fig. 9. Cascading risk of serial cases.

indices are ordered from the "most deterministic" index to the "most risk-based" index.

1) Worst-case index: The worst-case index is different for low voltage than it is for voltage instability.

- Low voltage: If there is one or more violations, risk = 1.0; otherwise, risk = 0.
- Voltage instability: It is given as the maximum value of the ratio Forecasted_Load/Loadability over all contingencies.

This index does not consider either form of uncertainty, it does not consider the severity level of the violation, and it does not reflect the number of violations.

2) Violation-count index: Here, we simply count the number of violations for a particular contingency. Violations for low voltage and for overloads are familiar. A voltage instability violation is defined as when the $\%margin$ falls below a prespecified level. This index does not consider either form of uncertainty, and it also does not consider the severity level of the violation, but it does reflect the number of violations.

3) Expected violations count index: This index is the summation over all contingencies of the contingency probability and the violation count for that contingency. So this index does not consider uncertainty in operating condition or the severity level of the violation, but it does account for the uncertainty in contingency, and it reflects the number of violations.

4) Expected violations (EV): This is the risk index using the discrete severity function. It does not consider the severity level of the violation, but it does account for the uncertainty in the contingency, and it additionally accounts for the uncertainty in the operating conditions.

5) Expected weighted violations (EWV): This is the risk index using the continuous severity function. It not only accounts for uncertainty in contingency and operating condition, but also reflects the severity of each violation.

The attributes of these indices are summarized in Table I.

We compute the five indices for low voltage and voltage instability, respectively, for all 18 operating cases, and we compare their information content.

A. Low-Voltage Risk

Fig. 10 shows the low voltage risk for the 18 cases for index 1 and index 4. From this figure, it is clear that the deterministic index 1 identifies cases 1, 2, 3, 5, 10, 11, 12, and 15 as equivalent, implying that each of these cases has at least one violation,

TABLE I
SUMMARY OF INDICES USED

Index Number	Uncertainty		Severity	
	In contingency?	In operating conditions	Number of violations?	Level of violations?
1	No	No	No	No
2	No	No	Yes	No
3	Yes	No	Yes	No
4	Yes	Yes	Yes	No
5	Yes	Yes	Yes	Yes

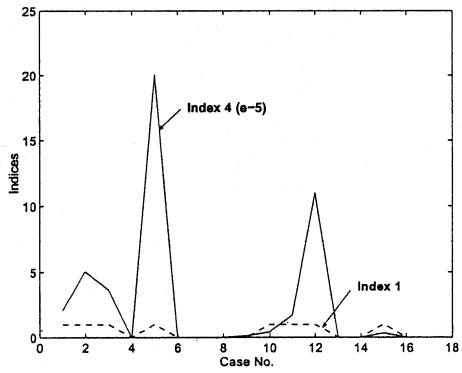

Fig. 10. Low-voltage risk for serial cases—1.

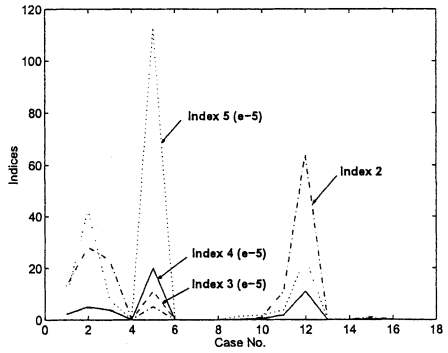

Fig. 11. Low-voltage risk for serial cases—2.

but the risk-based index 4 clearly shows significant differences between these cases.

To gain more appreciation for why these differences arise, Fig. 11 shows the low-voltage risk for the 18 cases for Indices 2–5. From this plot, we make the following observations:

- Comparison between indices 2 and 3 indicates the effect of modeling uncertainty in contingency. Index 2 identifies the most risky case as case 12, and it ranks case 5 as the fifth most risky among all cases. In considering the contingency probability, as does index 3, we see that cases 5 and 12 are identified as equally risky. The reason for this difference is relative to the results indicated by index 2 is that most of the violations in case 5 occur due to high-probability contingencies, whereas violations in other cases, although more numerous, occur from contingencies that are lower in probability.
- Comparison between the indices 3 and 4 indicates the effect of including uncertainty in operating condition. In case 5, for example, we see that index 4 results in significantly higher risk

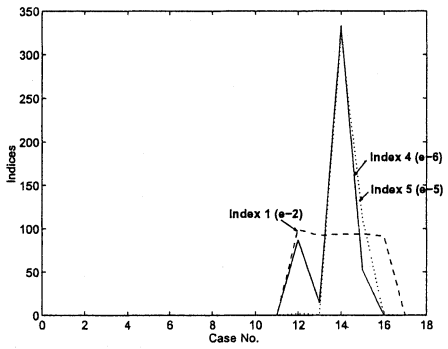

Fig. 12. Voltage instability risk for serial cases—1.

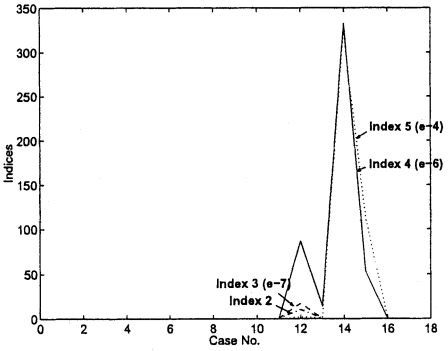

Fig. 13. Voltage instability risk for serial cases—2.

than index 3. The reason for this is that contingencies that are close to a violation reflect no risk in index 3, but they do in index 4 because of uncertainty in operating conditions.

B. Voltage Instability Risk

Fig. 12 shows the voltage instability risk for the 18 cases for indices 1, 4, and 5. From this figure, the deterministic index 1 shows that cases 12 to 16 all have a serious voltage instability problem. But after considering the probability of contingencies and the uncertainty of operating conditions (indices 4 and 5), the voltage instability risk of case 13 and case 16 is very low. So the decision made based on the deterministic index will be very conservative.

To gain more appreciation for why these differences arise, Fig. 13 shows the voltage instability risk for the 18 cases for iIndices 2–5. From index 3, we can see that in only one contingency in case 12 does the load exceed the loadability. In all other cases and contingencies, there is no such deterministic violation. But from indices 4 and 5 we can see that the case that has the most serious voltage instability problem is not case 12, but case 14. This is because in case 12, only one contingency has the voltage instability problem, in other contingencies, the loads are much less than the loadability. But in case 14, though there is no contingency having a deterministic violation, in all contingencies, the loads are very near the loadability. If we consider the uncertainty of the operating condition, part of the probability distribution of the load will exceed the loadability mean value. So case 14 has the most serious voltage instability problem.

VI. Discussion

Some salient features of OL-RBSA not available with the traditional, deterministic approach to control-room security-economy decision making are

- *Leading Indicator*: The risk index is a leading indicator for security level, in that assessment is done for the conditions under which the action is taken. It performs security assessment on a **near-future** condition.
- *Full Decision Space*: The modeling of severity function should not depend on a presupposed operator decision as this constrains the decision space, which is the space of investigation. LOLP, EUE, cost of redispatch, as indices for use in control room security-related decision making, each presuppose a decision and are therefore inappropriate.
- *Quantitative Index*: It provides a quantitative index that reflects security level in a condensed fashion. This not only allows efficient comprehensibility by the operator but also facilitates inclusion in formal decision-making paradigms.
- *Decomposability:* Since the index is decomposable, the index provides efficient means to quickly identify and investigate specific high-risk situations localized at any level.
- *More Complete Portrayal of Security Level*: OL-RBSA provides an assessment that appropriately reflects the additional risk from high-probability outages, from highly severe outages, from nonlimiting problems, and from uncertainty in future loading conditions.

We indicated in Section I that all of the work related to this paper is in support of a decision problem, and we referred to this decision problem as control room security-economy decision making. This decision problem is a continuous one that occurs in the control room to balance the level of security with the economic costs of achieving it. This problem has typically been addressed heuristically based entirely on the intuition of humans. We do not intend to eliminate the human involvement in this decision problem. However, we believe that there are tools that could significantly aid the human. Several such kinds of decision-making tools have been proposed [22]–[25]. Most of the methods that we have investigated are multicriteria decision-making (MCDM) methods. These methods generally require that each criterion used in the decision making be quantifiable. Thus, OL-RBSA enables security to be included in these decision-making methods. Other criterion includes variance, costs, and regret. Some of the methods that we have considered include risk-based optimal power flow, sensitivity-based methods, weighted MCDM, outranking methods such as ELECTRE IV, and methods based on evidential theory. We have yet to identify a single method that appears superior to all others, so we envision that we would produce a toolbox of methods, and that the solution(s) produced by each method would comprise a list of suggestions made to the operator. We believe that this is a very rich area of research made possible by OL-RBSA.

VII. Summary and Conclusions

OL-RBSA computes indices based on probabilistic risk for the purpose of performing online security assessment of high-voltage electric power transmission systems. The indices computed are for use by operators and operational engineers in the

control room to assess system security levels as a function of existing and near-future network conditions. Uncertainties in near-future loading conditions and contingency conditions are modeled. Severity functions are adopted to uniformly quantify the severity of network performance for overload and voltage security. The overload security indices include probabilistic expectations of the severity associated with high circuit flows and the severity associated with cascading overloads. The voltage security indices include probabilistic expectations of the severity associated with low bus voltages and the severity associated with voltage instability. OL-RBSA can provide high-level system or regional views of security and, when risk is high, allows the user to efficiently hone in on specific regions, components, problem types, or contingencies that cause or incur the risk, because the risk is decomposable.

Control-room security-economy decision making has recently taken on an increased level of visibility as a result of more frequently encountered stressed conditions. This trend drives the need for a quantitative measure that accurately reflects security level and can be used in formal decision-making paradigms. The index described in this paper is appropriate for this purpose, as it reflects risk. We believe that the use of this index will improve control-room security-economy decision making and, therefore, in the long run, result in more economically efficient energy supply at higher system reliability levels.

REFERENCES

[1] J. McCalley, A. Fouad, V. Vittal, A. Irizarry-Rivera, B. Agrawal, and R. Farmer, "A risk based security index for determining operating limits in stability-limited electric power systems," *IEEE Trans. Power Syst.*, vol. 12, pp. 1210–1217, Nov. 1997.

[2] A. Irizarry-Rivera, J. McCalley, and V. Vittal, "Computing probability of instability for stability constrained electric power systems," *Elect. Power Syst. Res.*, vol. 42, pp. 135–143, 1997.

[3] W. Fu, S. Zhao, J. McCalley, V. Vittal, and N. Abi-Samra, "Risk-based assessment for special protection schemes," *IEEE Trans. Power Syst.*, vol. 17, pp. 63–72, Feb. 2002.

[4] V. Vittal, J. McCalley, V. Van Acker, and N. Abi-Samra, "Transient instability risk assessment," in *Proc. IEEE Power Eng. Soc. Summer Meeting*, July 18–22, 1999, pp. 185–192.

[5] V. Van Acker, J. McCalley, V. Vittal, and J. Pecas-Lopes, "Risk-based transient stability assessment," in *Proc. Budapest Powertech Conf.*, Budapest, Hungary, Sept. 1999.

[6] CIGRE TF 38.03.12 (R. J. Marceau and J. Endrenyi, Chairmen), "Power system security assessment: A position paper," Electra, no. 175, pp. 48-78, Dec. 1997.

[7] M. Lifson and E. Shaifer, *Decision and Risk: Analysis for Construction Management*. New York: Wiley, 1982.

[8] The Instrument Society of America (ISA), "Application of safety instrumented systems for the process industries," Std., ISA S84.01, Feb. 1996.

[9] The Int. Electrotechnical Commission, "Functional safety of electrical/electronic/programmable electronic safety-related systems,", IEC-61508, Parts 1–7, Apr. 1998.

[10] The Int. Electrotechnical Commission, "Functional safety instrumented systems for the process industry sector," Std., IEC-61511, Parts 1–3, June 1999.

[11] J. Chen and J. McCalley, "Comparison between deterministic and probabilistic study methods in security assessment for operations," in *Proc. VI Int. Conf. Probabilistic Methods Applied to Power Syst.*, Madeira Island, Portugal, Sept. 2000, SA-090.

[12] J. McCalley, V. Vittal, H. Wan, Y. Dai, and N. Abi-Samra, "Voltage risk assessment," in *Proc. IEEE Power Eng. Soc. Summer Meeting*, Edmonton, AB, Canada, 1999.

[13] H. Wan, "Risk-based security assessment for operating electric power systems," Ph.D. dissertation, Iowa State University, Ames, 1998.

[14] A Berizzi, S. Corse, D. Dosi, P. Finazzi, P. Marannino, and S. Corsi, "First and second order methods for voltage collapse assessment and security enhancement," *IEEE Trans. Power Syst.*, vol. 13, pp. 543–551, May 1998.

[15] V. Ajjarapu and C. Christy, "The continuation power flow: A tool for steady state voltage stability analysis," *IEEE Trans. Power Syst.*, vol. 7, pp. 416–423, Feb. 1992.

[16] C. Canizares, F. Alvarado, C. L. DeMarco, I. Dobson, and W. F. Long, "Point of collapse and continuation methods for large ac/dc systems," *IEEE Trans. Power Syst.*, vol. 8, pp. 1–8, Feb. 1993.

[17] F. L. Alvarado, I. Dobson, and Y. Hu, "Computation of closest bifurcation in power systems," *IEEE Trans. Power Syst.*, vol. 9, pp. 918–928, May 1994.

[18] B. Lee and V. Ajjarapu, "Invriant Subspace Parametric Sensitivity (ISPS) of structure preserving power systems models," *IEEE Trans. Power Syst.*, vol. 11, pp. 845–850, May 1996.

[19] B. Long and V. Ajjarapu, "The sparse formulation of ISPS and its application to voltage stability margin sensitivity and estimation," *IEEE Trans. Power Syst.*, to be published.

[20] S. Greene, I. Dobson, and F. L. Alvarado, "Sensitivity of the loading margin to voltage collapse with respect to arbitrary parameters," *IEEE Trans. Power Syst.*, vol. 12, pp. 262–272, Feb. 1997.

[21] S. R. Searle, *Linear Models*. New York: Wiley, 1971, pp. 40–44.

[22] J. McCalley and M. Ni, "Decision-making for security-constrained power systems," Electric Power Research Institute, Final Rep. for EPRI Project WO721 201, Aug. 2000.

[23] H. Wan, J. McCalley, and V. Vittal, "Decision making under risk," in *Proc. North American Power Conf.*, Cleveland, OH, Oct. 1998, pp. 428–433.

[24] V. Van Acker, J. McCalley, and M. Matos, "Multiple criteria decision making using risk in power system operation," in *Proc. VI Int. Conf. Probabilistic Methods Applied to Power Syst.*, Madeira Island, Portugal, Sept. 2000, PSO2-127.

[25] M. Ni and J. McCalley, "Risk-based preventive/corrective action selection—Multi-criteria decision making by the method of evidential theory," in *Proc. of the VI Int. Conf. Probabilistic Methods Applied to Power Syst.*, Madeira Island, Portugal, Sept. 2000.

Ming Ni (M'98) received the B.S. and Ph.D. degrees from Southeast University, China, in 1991 and 1996, respectively.

Currently, he is a Postdoctoral Researcher in Iowa State University, Ames.

James D. McCalley (SM'97) received the B.S., M.S., and Ph.D. degrees from Georgia Institute of Technology, Atlanta, in 1982, 1986, and 1992, respectively.

Currently he is an Associate Professor in the Electrical and Computer Engineering Department at Iowa State University, Ames, where he has been since 1992. He was with Pacific Gas and Electric Company from 1986 to 1990.

Vijay Vittal (F'97) received the B.E. degree in electrical engineering from Bangalore, India, in 1977, the M.Tech. degree from the India Institute of Technology, Kanpur, India, in 1979, and the Ph.D. degree from Iowa State University in 1982.

Currently, he is a Professor in the Electrical and Computer Engineering Department at Iowa State University, Ames.

Dr. Vittal is the recipient of the 1985 Presidential Young Investigator Award.

Tayyib Tayyib (M'95) received the B.S. degree in electrical engineering from the University of Peshawar, Pakistan, in 1967, and M.S. degree in electrical engineering from the University of Wisconsin, Milwaukee, in 1997.

Currently, he is Project Manager of Grid Operations and Planning at Electric Power Research Institute, Palo Alto, CA, where he has been since 1999. He specializes in computational aspects of power system analysis and software development.